AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method of authenticating an optical channel comprising:

modulating optical pulses corresponding to a first bit sequence based on a second bit sequence;

transmitting the optical pulses over the optical channel;

receiving the modulated optical pulses;

demodulating the received optical pulses using the second bit sequence; [[and]]

authenticating the optical channel based on a number of bits from the first bit sequence that are correctly received and demodulated;

calculating a message authentication code based on a block of text; and

deriving the first and second bit sequences from the message authentication code.

2. (original) The method of claim 1, wherein every bit in the first bit sequence is identical.

3. (original) The method of claim 1, wherein the first bit sequence is a pseudo-random bit sequence.

4. (original) The method of claim 1, wherein the second bit sequence is a pseudo-random bit sequence.

5. (original) The method of claim 1, wherein the optical pulses are modulated using polarization modulation.

6. (original) The method of claim 5, wherein each bit of the first bit sequence specifies one of two possible polarizations to apply to the optical pulses.

7. (original) The method of claim 5, wherein each K bits of the second bit sequence, where K is a positive integer, specifies a polarization to apply to the optical pulses.

8. (original) The method of claim 6, wherein each bit of the first bit sequence specifies either a vertical or horizontal polarization.

9. (original) The method of claim 1, wherein the optical pulses are modulated using phase modulation.

10. (original) The method of claim 9, wherein each bit of the first bit sequence specifies one of two possible phases to shift the optical pulses.

11. (original) The method of claim 9, wherein each K bits of the second bit sequence, where K is a positive integer, specifies a phase to shift the optical pulses.

12. (original) The method of claim 1, wherein authenticating the optical channel includes:

tabulating the number of bits from the first bit sequence that are correctly received;

tabulating the number of bits from the first bit sequence that are incorrectly received; and

authenticating the optical channel when the tabulated number of correctly received bits expressed as a fraction of a total number of correctly and incorrectly received bits is greater than a threshold value.

13. (original) The method of claim 1, wherein the first bit sequence and the second bit sequence are derived from shared secret keys.

14. (original) The method of claim 1, wherein the second bit sequence is distributed as a shared secret key and the first bit sequence is distributed as a known sequence.

15. (original) The method of claim 1, further comprising:

computing a message authentication code based on communications over a public channel; and

deriving at least one of the first and second bit sequences based on the message authentication code.

16. (canceled)

17. (original) The method of claim 1, further comprising:

sharing the second bit sequence over a public channel,

wherein authenticating the optical channel further includes

transmitting a representation of the demodulated and received optical pulses to an entity that transmitted the optical pulses over the optical channel, and

comparing the first bit sequence to the representation of the demodulated and received optical pulses.

18. (currently amended) A method comprising:

calculating a message authentication code based on a block of text;

deriving first and second bit sequences from the message authentication code;

receiving optical pulses corresponding to [[a]]the first bit sequence that were modulated based on [[a]]the second bit sequence, the optical pulses being received over an optical channel;

demodulating the received optical pulses using the second bit sequence; and

authenticating the optical channel based on a number of bits from the first bit sequence that are correctly received and demodulated.

19. (original) The method of claim 18, wherein the optical pulses are modulated using polarization modulation.

20. (original) The method of claim 19, wherein each bit of the first bit sequence specifies either a vertical or horizontal polarization.

21. (original) The method of claim 18, wherein the optical pulses are modulated using phase modulation.

22. (original) The method of claim 18, wherein the first bit sequence and the second bit sequence are distributed as shared secret keys.

23. (original) The method of claim 18, wherein the second bit sequence is distributed as a shared secret key and the first bit sequence is a known sequence.

24. (original) The method of claim 18, further comprising:

computing a message authentication code based on communications over a public channel; and

deriving at least one of the first and second bit sequences based on the message authentication code.

25. (currently amended)A cryptographic device comprising:

a polarized pulse generator configured to emit optical pulses polarized in one of a first state and a second state based on values stored in a first bit sequence; and

a polarizing rotator configured to rotate the optical pulses received from the polarized pulse generator by an angle specified by one or more bits from a second bit sequence to obtain a series of modulated optical pulses,

wherein the optical pulses are transmitted over an optical channel and used to authenticate the optical channel, and

wherein the first and second bit sequences are derived from a calculated message authentication code, the calculation based on a block of text.

26. (original) The device of claim 25, wherein the polarized pulse generator further comprises:

a first laser configured to emit a horizontally polarized optical pulse when a bit in the first bit sequence specifies the first state; and

a second laser configured to emit a vertically polarized optical pulse when the bit in the first bit sequence specifies the second state.

27. (original) The device of claim 25, wherein each bit of the first bit sequence specifies either a vertical or horizontal polarization.

28. (original) The device of claim 25, wherein the first bit sequence and the second bit sequence are distributed as shared secret keys.

29. (original) The device of claim 25, wherein the second bit sequence is distributed as a shared secret key and the first bit sequence is distributed as a known sequence.

30. (original) The device of claim 25, further comprising:

computing a message authentication code based on communications over a public channel; and

deriving at least one of the first and second bit sequences based on the message authentication code.

31. (currently amended) A cryptographic device comprising:

a polarization rotator configured to rotate optical pulses received over an optical channel by an angle specified by one or more bits from a second bit sequence; and

a polarizing beam splitter configured to receive the optical pulses rotated by the polarization rotator ;

a detector configured to generate indications of the polarizations of the received optical pulses; and

a counter configured to tabulate a number of times the detector indicates that the received optical pulses are polarized in a state that matches a state of a corresponding bit in a first bit sequence,

wherein the optical channel is authenticated based on at least one count value of the counter, and

wherein the first and second bit sequences are derived from a calculated message authentication code, the calculation based on a block of text.

32. (original) The device of claim 31, wherein the counter is further configured to tabulate a number of times the detector indicates that the received optical pulses are polarized in a state that does not match the state of the corresponding bit in the first bit sequence.

33. (original) The device of claim 31, wherein each bit of the first bit sequence specifies either a vertical or horizontal polarization.

34. (original) The device of claim 31, wherein the first bit sequence and the second bit sequence are distributed as shared secret keys.

35. (original) The device of claim 31, wherein the second bit sequence is distributed as a shared secret key and the first bit sequence is distributed as a known sequence.

36. (original) The device of claim 31, further comprising:

computing a message authentication code based on communications over a public channel; and

deriving at least one of the first and second bit sequences based on the message authentication code.

37. (currently amended) A cryptographic device comprising:

phase setting logic configured to determine an initial phase based on values stored in a first bit sequence;

summing logic configured to add the initial phase to a second phase determined based on one on or more bits from a second bit sequence and to output a summed phase angle; and

a phase modulator configured to modulate optical pulses by the summed phase angle to obtain a series of modulated optical pulses,

wherein the modulated optical pulses are transmitted over an optical channel and used to authenticate the optical channel, and

wherein the first and second bit sequences are derived from a calculated message authentication code, the calculation based on a block of text.

38. (original) The device of claim 37, further comprising:

a photon source configured to generate the optical pulses.

39. (original) The device of claim 37, wherein the first bit sequence and the second bit sequence are distributed as shared secret keys.

40. (original) The device of claim 37, wherein the second bit sequence is distributed as a shared secret key and the first bit sequence is distributed as a known sequence.

41. (original) The device of claim 37, further comprising:

logic configured to compute a message authentication code based on communications over a public channel; and

logic configured to derive at least one of the first and second bit sequences based on the message authentication code.

42. (currently amended) A device comprising:

means for calculating a message authentication code based on a block of text;

means for deriving first and second bit sequences from the message authentication code;

means for receiving optical pulses corresponding to [[a]]the first bit sequence that were modulated based on [[a]]the second bit sequence, the optical pulses being received over an optical channel;

means for demodulating the received optical pulses using the second bit sequence; and

means for authenticating the optical channel based on a number of bits from the first bit sequence that are correctly received and demodulated.